Research and Design of Network Behavior Management System Based on B/S Architecture

Deng XinXin Qiu ZhongPan Yang Xiaofang
Xiamen University, Cognitive Science Department, Fujian Key Laboratory of the Brain-like Intelligent Systems
Xiamen, China, 361005

***Abstract*—with the rapid development of Internet and information technology, network office, network education, paperless office has become increasingly popular. Computers and network have become the effective and essential tools of schools, families and enterprises. However, with the popularity of Internet behavior in a work or study environment, the problem that students and employees use the computer and network to do something unrelated with study and work become more and more serious, what's more, children may be misled to visit junk websites. The abuse of computers and network is widespread in enterprises as well. Hence, it is important to build an effective network behavior management system to monitor and manage the internal network hosts behavior.**

We put forward a network behavior management system based on B/S architecture. Our research facets are as follows:: According to the function of the system and architecture, the system is divided into three layers: Client Management UI layer, Sever layer, Data Memory layer. We have integrated a variety of Monitoring and Management technology and Protocol Analysis technology into the system. The paper first introduce the B/S architecture and compare with the C/S architecture, then detail the system construction, design of three modules, the work flow of the system, and the main functions of the network behavior management. At last, we conclude the prospect of the network behavior management system based on B/S architecture with HTML5 [1].

***Key words*— B/S Architecture, network behavior**

I. INTRODUCTION

At present, as the increase of people's awareness of network management, much network management software comes to our eyes. However, most of the network management software is based on C/S structure so the technical framework of software is mainly for the LAN applications. Because of rapid response, UI personalization and rapid adaptation to the complex process, applications based on C/S structure were very popular. With the development of internet, collectivization of enterprises and the establishment of enterprise branch offices, people's demand for the network management software is continually expanding and deepening. The increasing popularity of information and the further applications of management software make diversified network management software the more concerned. Besides cooperative partners, channels and mobile working increasing continually, the growing of enterprise branch offices makes the demand for distributed deployment and centralized management become more and more strong. It is more and more important for enterprises that getting network information in anytime in anywhere. B/S architecture has the unique advantages to meet enterprise in those facets.

II. B/S ARCHITECTURE

B/S architecture (Browser/Server) is a network model with the growing up of Web and the Web Browser is one of the most important applications of client. This model which focuses the core part of system on the server not only unifies the client but simplifies the development, maintenance and use of system. Just install a Browser such as Internet Explorer, Fire Fox on the client and the server installs the database. Browser interacts to the database by the web server. The biggest advantages of the B/S is that you can operate anywhere without having to install any special software, as long as there is a computer with Internet access or even a mobile phone supporting the browser, and the client is zero-maintenance. Using AJAX [2], the system greatly reduces the burden on the server, increases the interaction and is capable of local real-time refresh.

B/S architecture divides the data processing into three parts:

- Client initials the data request.
- Server receives the request and accesses to the database. The database executives the relevant command.
- Server processes the data and then sends back to the client.

Actually, the three layers B/S architecture separates the Transaction Processing Module from the client and integrates the module into the server, which is different from the two layers C/S architecture. As shown in Figure 1.

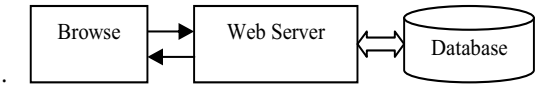

Figure 1. Three layers of the B/S architecture

III. DESIGN OF NETWORK BEHAVIOR MANAGEMENT SYSTEM

This system is installed on the server which is the export of LAN. Managers can use the browser by a terminal which is connected to the network to open and login the management system to monitor and manage the network behavior of computers in the LAN. The overall layout of the system is shown in Figure 2.

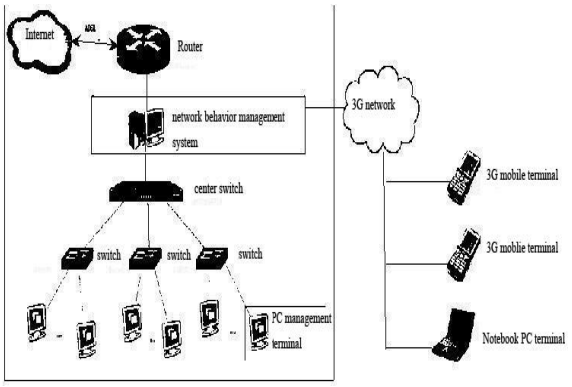

Figure 2. Overall layout of network behavior management system

A. *Client Management UI layer*

Client Management UI layer makes the functions provided friendly and easy to use. When the administrator logins the system, he/she can monitor and manage computers in LAN by the provided functional modules. The modules respond the administrator by AJAX module sending the request to the server. When AJAX module successfully received the response from the server, the module which sent the request locally refreshes related interfaces. Meanwhile, AJAX module updates some data which must be kept pace with the server in real time, such as computers information in LAN, network flow, etc.

This layer runs in Browser, so we use the JavaScript language [3] which is different levels supported by the Browser vendors. Fortunately, many third party Frameworks which almost solve the different between the Browsers have been designed. So we used the EXT [4] JavaScript Framework to implement our UI layer.

Figure 3 shows the some part of Client Management UI layer.

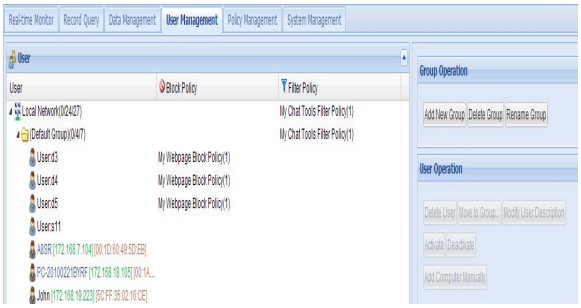

Figure 3. Part of Client Management UI layer

B. *Server layer and Data Memory layer*

Server layer is the second layer, in which, the functional modules provided to administrators are actually operated. Server layer sends the computed data to the Client UI layer, and then Client UI layer renders the data and refreshes the related part just as functional modules run in the Browser.

Data Memory as the third layer includes two databases. One is the application database which mainly stores the important data such as computers in LAN, policies formulated by administrators, system information, etc. Second is the log database which stores a variety of violation, statistical reports and other information.

IV. FUNCTIONAL MODULES OF NETWORK BEHAVIOR MANAGEMENT SYSTEM

Administrator Authentication: This module requires the administrator to enter the account and the password, and then encodes the input to send to the server which will check the validity.

User Management: The module presents computers in LAN to the administrator in a tree view which uses the MAC and the IP of computers as the main or default identifier. It allows administrator to change the description of computers to make operation easier. Administrator can delete computers which don't need to be monitored and managed. Besides, administrator can group computers, so administrator can make policies to the group, and the computers in the same group will shared the same policies.

Policy Management: In this module, administrator can make policies such as setting block, filter, alarm and user-defined monitoring item. It also allows administrator set the policy duty time which means the policy will work in the duty time. For example, administrator can make the policy work in working hours while allowing employees to surf the net for entertainment. A policy setting is shown in Figure 4.

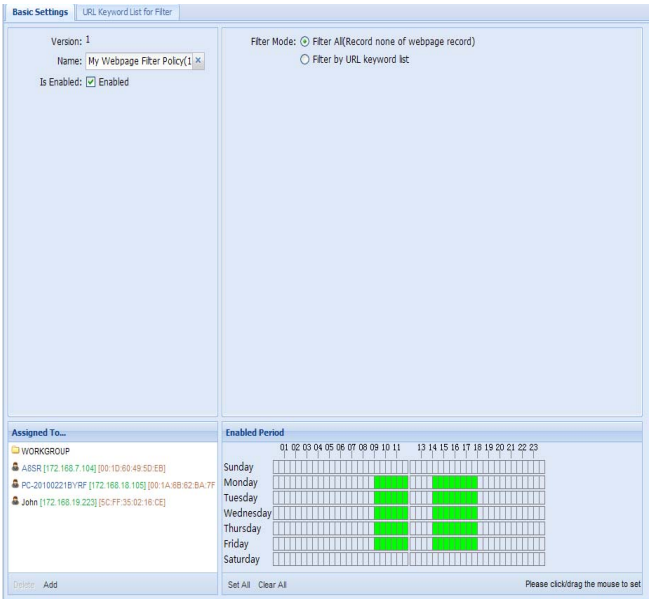

Figure 4. A policy setting

Network Management: The main monitor and management function of the system are integrated in this module. It manages the network automatically according to policies that the administrator made. This module contains some sub modules as follows:

- Real-time Monitor: It monitoring the network traffic in real time helps administrator analyze whether the existing bandwidth resources can meet the needs of the business. When congestion occurs, it can quickly examine the computers which cause the abnormal traffic. It has some other functions such as visually observing the total flow of uplink and downlink, dynamic displaying the trend of network in recent

time to understand the variation of the bandwidth peaks and troughs.

- Network Behavior Monitor: The functions of the module are as follows: monitoring the pages of computers recently visited, while providing cached pages to keep the records to examine whether violating the management policies; monitoring the mails sent by computers, including mails body and attachments; monitoring the chat tools and the files transferred by the tools such as MSN to avoid disclosure of enterprises' sensitive information; monitoring whether the behavior of computers are not work-related in working hours such as playing games, downloading, watching the video online, etc.
- Web Filtering: It uses the pre-classification of web filtering technology and the flexible policy settings to filter the contents which violate the national law and against the enterprise security, which avoid consciously or unconsciously visiting web pages include the illegal contents. It can set flexible policy to meet the needs of individual management of business for computers, time, web category, URL keyword, file type and other conditions.
- Application Control: It can block the BT, eMule and other P2P software, distinguish the mainstream chat tools such as MSN, and control the online video like Youtube and streaming media applications like Win Media, Real Media.
- Content Audit: This module can restore and audit the mails sent and received, which includes time, title, mailing address, content and attachments; completely record the contents of chats and file transfers by chat tools and support to query the details of chat.
- Bandwidth Management: Administrator can set the limit flow for groups and computers to reasonably assign the bandwidth resources.

Log Management: This module supports independent optional log center which stores the history log of administrator. The log capacity depends on the size of the physical space. However, it can achieve mass storage by expansion of hard drive, which protects the integrity and security of log data. It also provides a complete and fine-grained query which covers the monitoring and application information.

System Management: Administrator chooses the network card to be monitored, sets the interface language, watches the working state of engines, and sets the working parameters of engines.

Collector: This module which runs in background collects the computers information in LAN. The information of a computer includes MAC, IP, CPU, Hard disk and so on. A computer is considered as two computers if it has two network cards. Collector runs in every interval time which can be set by the administrator. If Collector finds information of a computer changed, then it updates the application database. Of course, the Client requests the data will be kept the latest.

Anomaly Detection: This module also runs in background so it will continue working. It devises a set of statistical metrics which model the behavior of an entity, usually a user, user groups or a host computer. The profile of a user entity for instance, may include information such as web pages visited, files transferred, the amount of bytes transmitted in both directions, the chat logs made by the chat tools, the time of day or the terminals he usually login from, etc. The profile of a host computer may include the average CPU utilization, the total flow passed, the number of login users, and so on. The anomaly detection module monitors the behavior of a computer, and constantly compares the policies made. In case it detects a deviation from the normal behavior it makes the appropriate measures according with the policies such as signals an alarm to the system security officer, blocks the abnormal behavior.

The functional modules which can extend along with the development of the monitoring technology have good extensibility. The part of modules structure is show in Figure 4, and the work flow chart of the system is show in Figure 5.

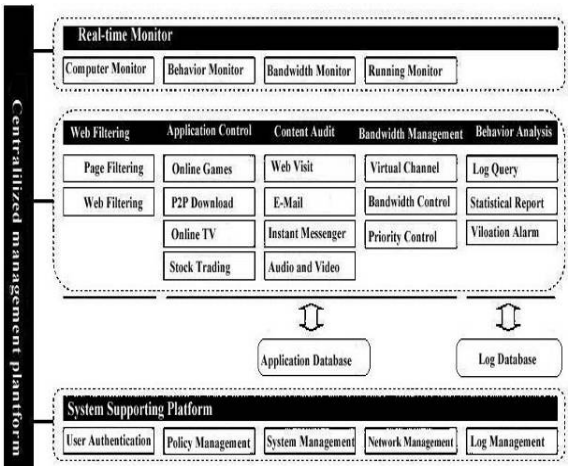

Figure 5. Part of modules structure

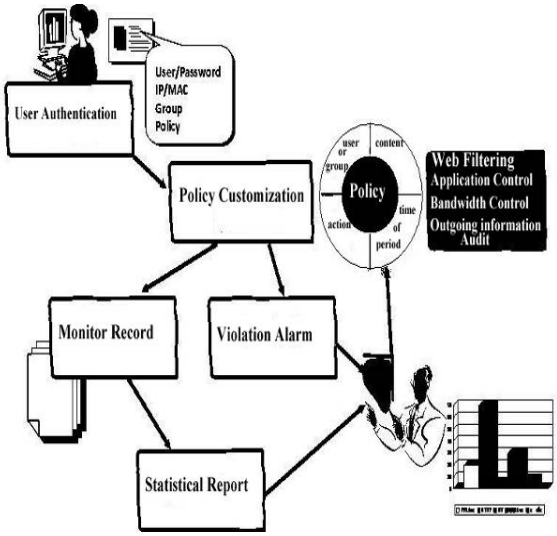

Figure 6. Work flow chart of the system

V. CONCLUSIONS – FUTURE WORK

The applications based B/S architecture compensate some faults that in the applications based C/S. B/S model which gradually becomes the main network system architecture has

been applied to the various design of systems. The network behavior management system based on B/S architecture gets a good application in the actual, which saves the cost for the enterprise and improves the efficiency of maintenance and upgrades. More important, with the development of HTML5 and the mobile network, monitoring and managing network by a mobile phone in anytime and anywhere will become reality.

We have finished the design of the system, however, in which, Client UI is designed with HTML4 and JavaScript, which may caused the mobile phone can't use the system perfectly. Future work includes the implementation of Client UI with HTLM5 and JavaScript, which will more perfectly support the mobile phone browser.

ACKNOWLEDGMENT

Special thanks to Xiamen ChengChuang Technology Co.ltd for their help in this project, especially thanks to Mr Zhijian Huang, YaNan Zhao and Fuliang Tong.

REFERENCES

[1] http://www.w3.org
[2] Jesse James Garrett "Ajax: A New Approach to Web Applications" http://www.adaptivepath.com/ideas/e000385
[3]http://en.wikibooks.org/wiki/Programming:JavaScript:Introduction
[4] Willebeek LeMair,M.H.and A.P.Reeves. Strategies for dynamic load balancing on highly parallel computers[J], IEEE Transaction Parallel and Distributed Systems. 1993, 4(9).979-993
[5]Coit C J, Staniford S. Toward Faster String Matching for Intrusion Detection or Exceeding the Speed of Snort[C]. Proc. of the DISCEX. 2001
[6] Aho A, Corasick M.Efficient String Matching an Aid to Biblio graphic Search [J].Communication of the ACM.1975, 18(6).333-340
[7]Nicholas C. Zakas. Professional JavaScript for Web Developers. Second Edition. POSTS & TELECOM PRESS, 2010
[8]Panagiotis Astithas,Giorgos Koutepas, Basil Maglaris. "Integrating Intrusion Detection and Network Management". Integrating Intrusion Detection and Network Management.
[9]Harvey M.Deitel . Java Web Services for Experienced Programmers. Pearson Education